

FIG. 1

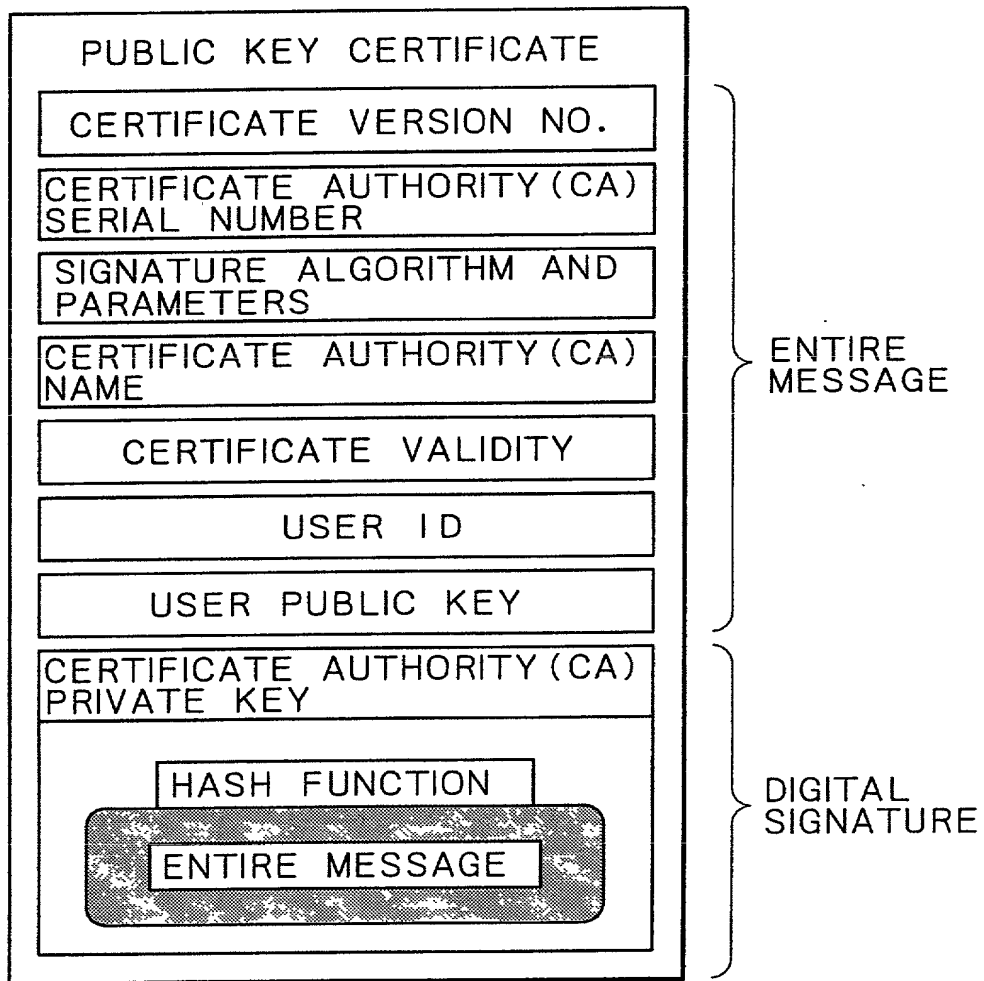


FIG. 2

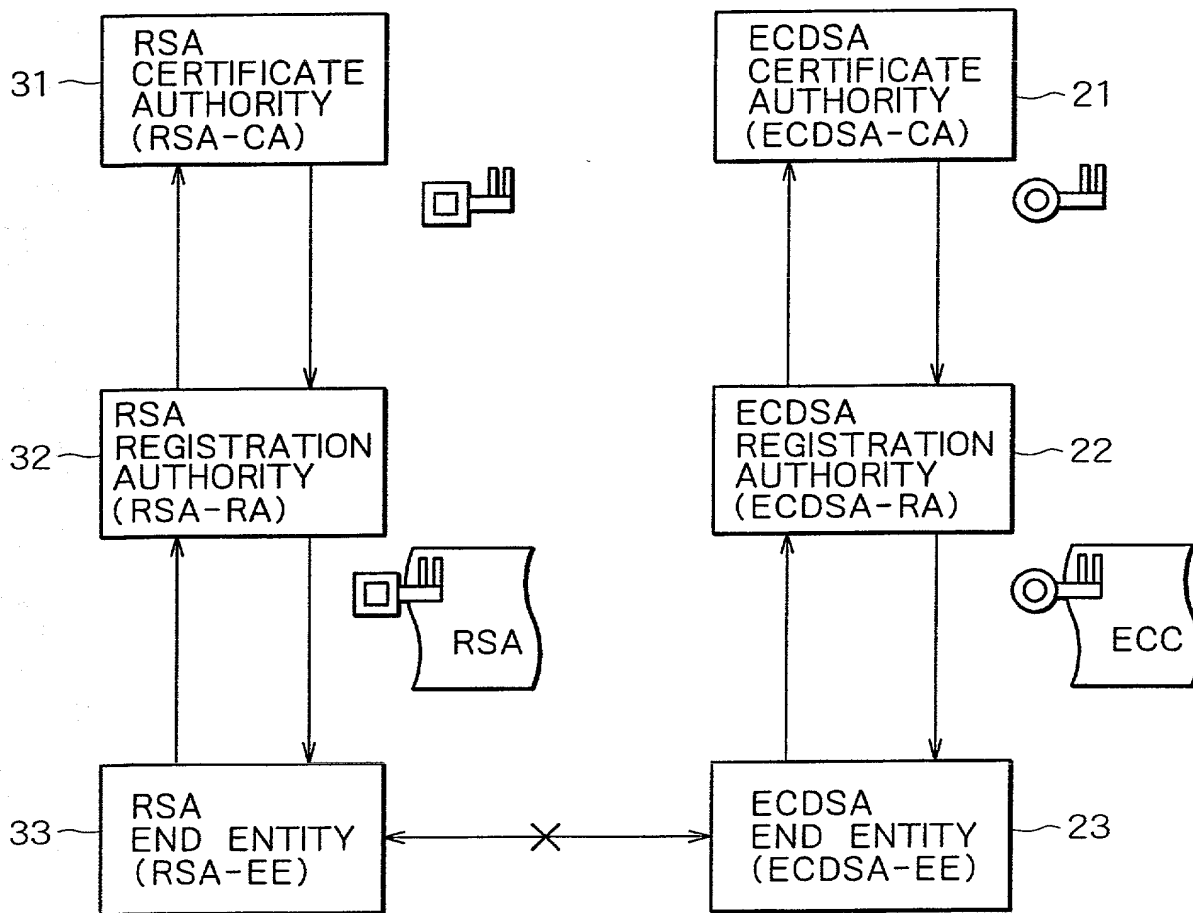


FIG. 3

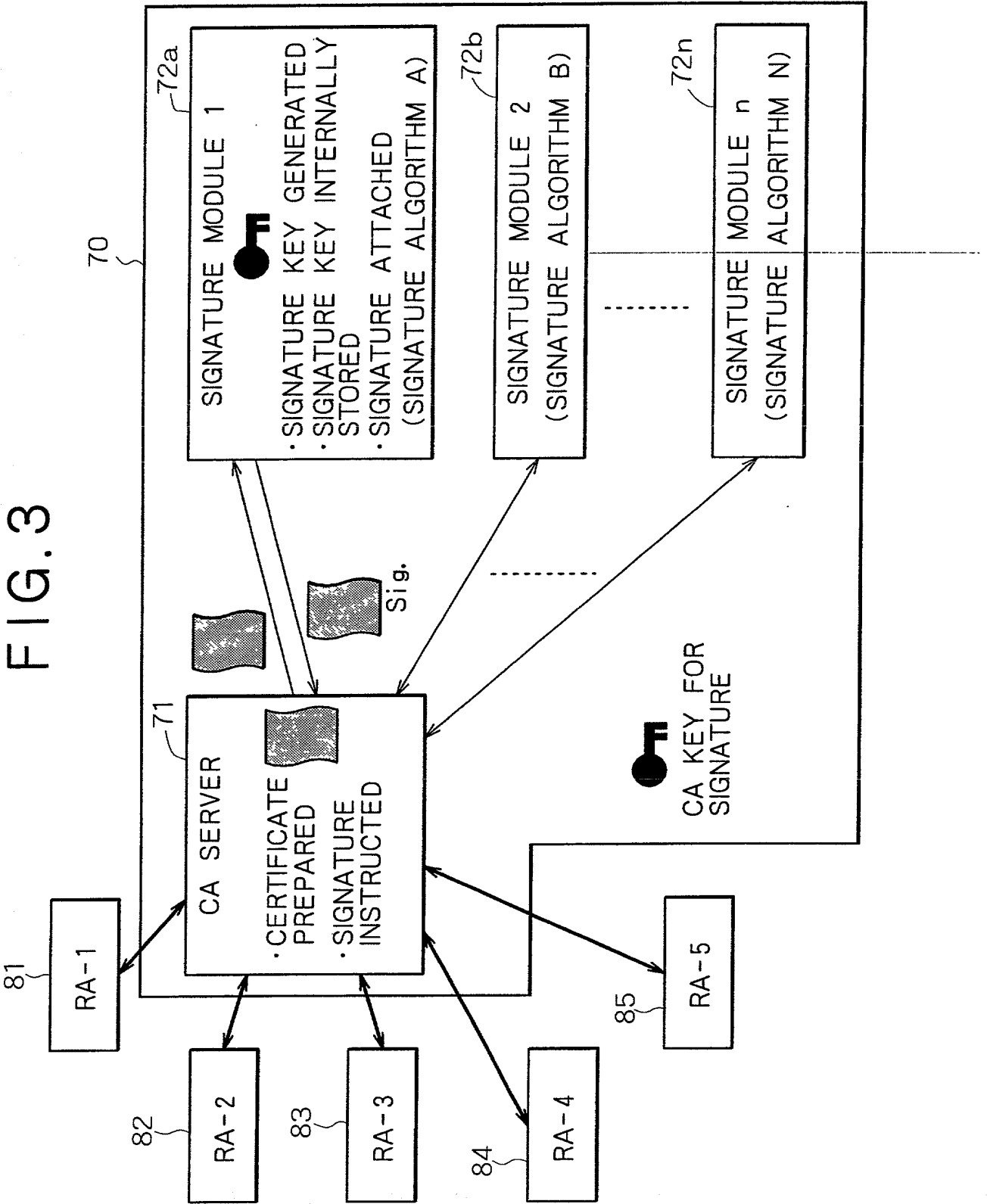


FIG. 4

EXAMPLE OF CERTIFICATE FORMAT (BASED ON X.509 V3)

ITEMS	DESCRIPTION	SETTINGS WITH THIS IA
Version 1		
version	VERSION OF CERTIFICATE FORMAT	V3
serial Number	CERTIFICATE SERIAL NUMBER FURNISHED BY IA	SEQUENTIAL SERIAL NUMBER
signature.algorithm Identifier algorithm parameters	CERTIFICATE SIGNATURE ALGORITHM AND PARAMETERS	• ELLIPTIC CURVE CRYPTOGRAPHY OR RSA • PARAMETERS IN THE CASE OF ELLIPTIC CURVE CRYPTOGRAPHY • KEY LENGTH IN THE CASE OF RSA
issuer	IA NAME (DISTINGUISHED NAME FORMAT)	NAME OF THIS IA
validity notBefore notAfter	VALIDITY OF CERTIFICATE • STARTING DATE AND TIME • ENDING DATE AND TIME	
subject	USER IDENTIFICATION NAME	USER DEVICE ID OR SERVICE ENTITY ID
subject Public Key Info algorithm subject Public key	USER'S PUBLIC KEY INFORMATION • KEY ALGORITHM • PUBLIC KEY	• ELLIPTIC CURVE CRYPTOGRAPHY OR RSA • USER'S PUBLIC KEY
Version 3		
authority Key Identifier key Identifier authority Cert Issuer authority Cert Serial Number	• KEY IDENTIFIER FOR SIGNATURE VERIFICATION BY IA • KEY ID NUMBER (OCTAL) • IA NAME (GENERAL NAME FORMAT) • CERTIFICATE SERIAL NUMBER	
subject key Identifier	APPLICABLE WHERE MULTIPLE KEYS NEED TO BE CERTIFIED	NOT USED
key usage (0) digital Signature (1) non Repudiation (2) key Encipherment (3) data Encipherment (4) key Agreement (5) key CertSign (6) cRL Sign	THE PURPOSE OF KEY USAGE IS DESIGNATED (0) FOR DIGITAL SIGNATURE (1) FOR REPUDIATION PREVENTION (2) FOR KEY ENCRYPTION (3) FOR MESSAGE ENCRYPTION (4) FOR DISTRIBUTION OF COMMON KEY (5) FOR VERIFICATION OF SIGNATURE ON CERTIFICATE (6) FOR VERIFICATION OF SIGNATURE ON CERTIFICATE REVOCATION LIST	USAGE (0), (1), (4) AND (6) APPLY
private Key Usage Period notBefore notAfter	USAGE PERIOD OF USER'S PRIVATE KEY	USAGE PERIOD OF CERTIFICATE=USAGE PERIOD OF PUBLIC KEY=USAGE PERIOD OF PRIVATE KEY (DEFAULT)

20250704 19:54:00

FIG. 5

policy Mappings issuer Domain Policy subject Domain Policy	NECESSARY ONLY WHEN CA IS CERTIFIED. AN ISSUER DOMAIN POLICY AND A SUBJECT DOMAIN POLICY ARE DEFINED.	NONE BY DEFAULT
supported Algorithms algorithm Identifier intended Usage intended Certificate Policies	ATTRIBUTES OF THE DIRECTORY (X.500) ARE DEFINED. WHEN THE OPPOSITE PARTY OF COMMUNICATION IS TO USE DIRECTORY INFORMATION, THAT PARTY IS INFORMED OF THE DIRECTORY ATTRIBUTES IN ADVANCE.	NONE BY DEFAULT
subject Alt Name	USER'S ALTERNATIVE NAME (GENERAL NAME FORMAT).	NOT USED
issuer Alt Name	THIS FIELD IS INCLUDED (NONE BY DEFAULT).	NONE BY DEFAULT
subject Directory Attributes	USER'S ANY ATTRIBUTES.	NOT USED
basic Constraints cA path Len Constraint	THIS FIELD SPECIFIES WHETHER THE PUBLIC KEY SUBJECT TO CERTIFICATION IS TO BE SIGNED BY THE CERTIFICATE AUTHORITY (CA) OR USED BY THE USER.	USED BY USER BY DEFAULT
name Constraints permitted Subtrees base minimum maximum excluded Subtrees	USED ONLY WHEN THE SUBJECT IS CA (CA CERTIFICATION).	NONE BY DEFAULT
policy Constraints require Explicit Policy inhibit Policy Mapping	DESCRIBED HERE ARE CONSTRAINTS REQUIRING EXPLICIT POLICY IDs AND INHIBIT POLICY MAPPING FOR THE REMAINING CERTIFICATION PATHS.	
CRL Distribution Points	DESCRIBED HERE ARE POINTS AT WHICH THE USER REFERENCES THE CERTIFICATE REVOCATION LIST (CRL) TO SEE WHETHER THE CERTIFICATE IS REVOKED.	THESE POINTS SERVE AS POINTERS INDICATING WHERE THE CERTIFICATE IS REGISTERED. THE CERTIFICATE REVOCATION LIST IS MANAGED BY THE ISSUER.
SIGNATURE	ISSUER'S SIGNATURE	

FIG. 6

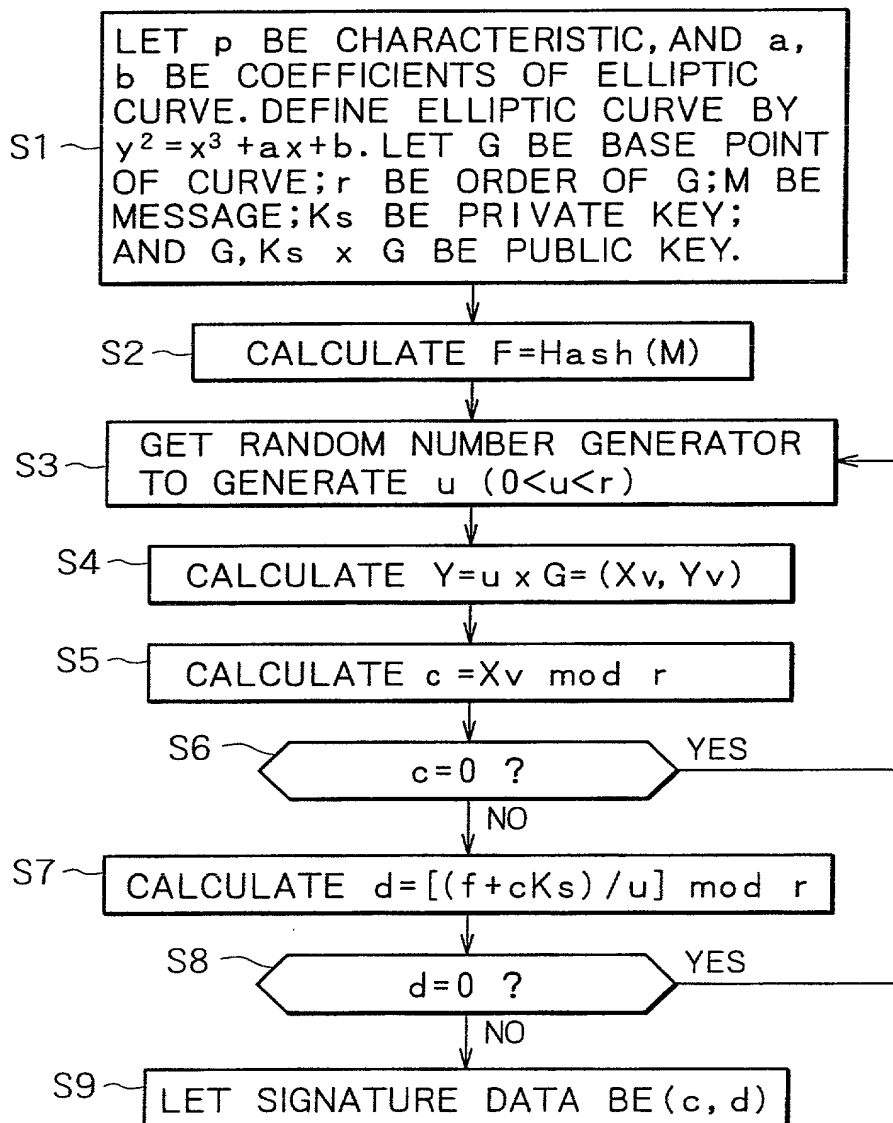


FIG. 7

LET p BE CHARACTERISTIC, AND a , b BE COEFFICIENTS OF ELLIPTIC CURVE. DEFINE ELLIPTIC CURVE BY $y^2 = x^3 + ax + b$. LET G BE BASE POINT OF CURVE; r BE ORDER OF G ; M BE MESSAGE; (c, d) BE SIGNATURE; AND $G, K_s \times G$ BE PUBLIC KEY.

S11

S12 $0 < c < r$ AND $0 < d < r$?

NO

YES

S13 CALCULATE $f = \text{Hash}(M)$

S14 CALCULATE $h = 1/d \bmod r$

S15 CALCULATE $h_1 = fh \bmod r$
AND $h_2 = ch \bmod r$

S16 CALCULATE POINT $P = (X_p, Y_p) = h_1 \times G + h_2 \cdot K_s \times G$

S17 IS P INFINITE POINT ?

YES

NO

S18 DOES $c = X_p \bmod r$ HOLD ?

NO

YES

S19 SIGNATURE VALID

S20

SIGNATURE INVALID

FIG. 8

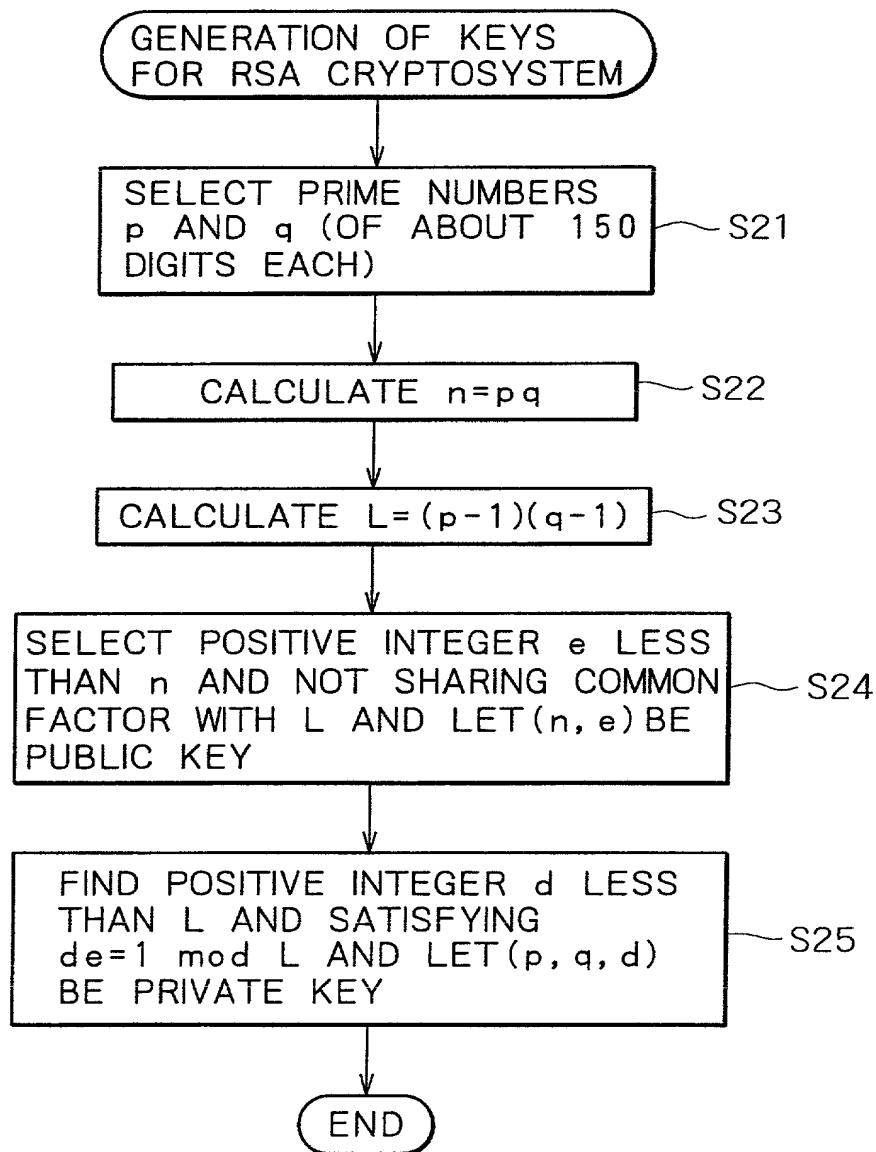


FIG. 9A

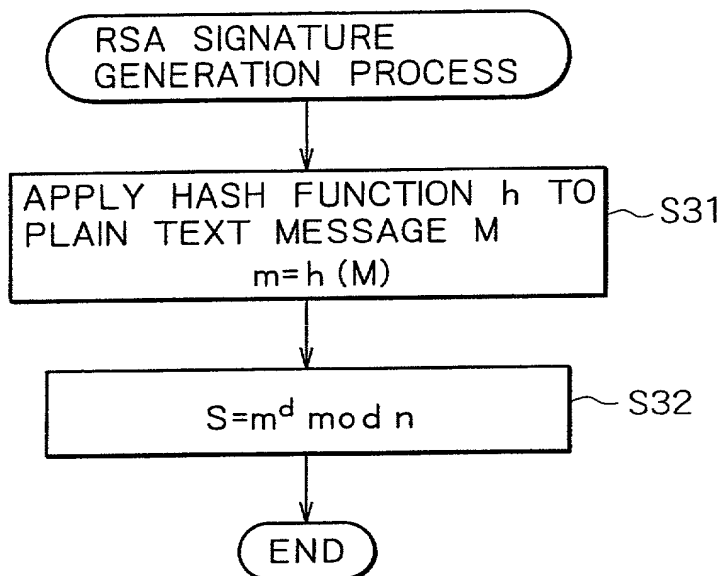


FIG. 9B

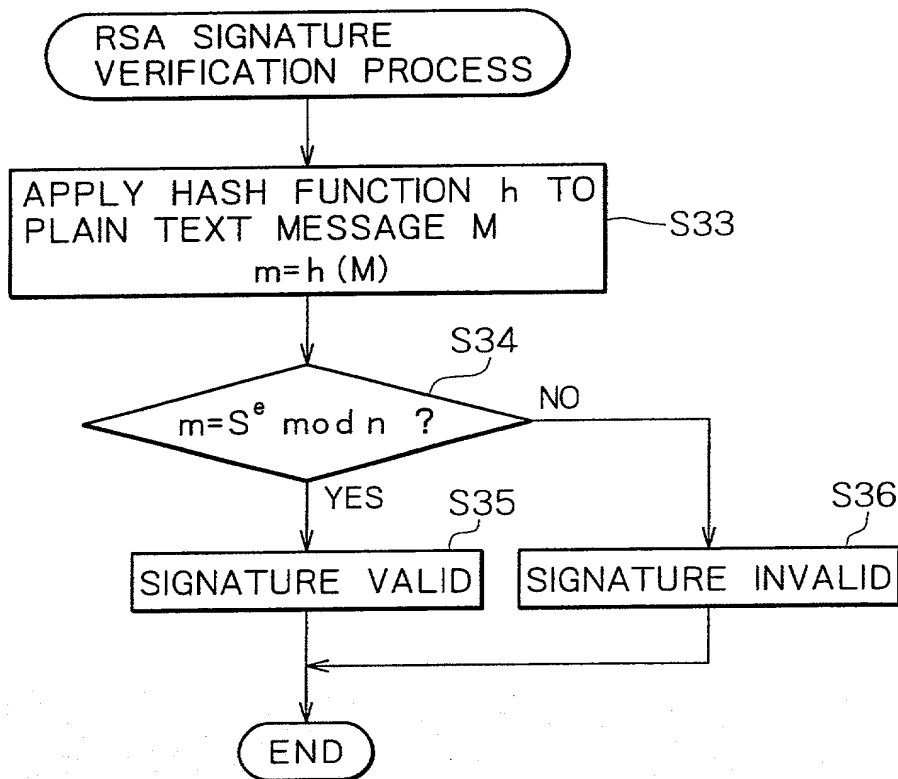


FIG. 10

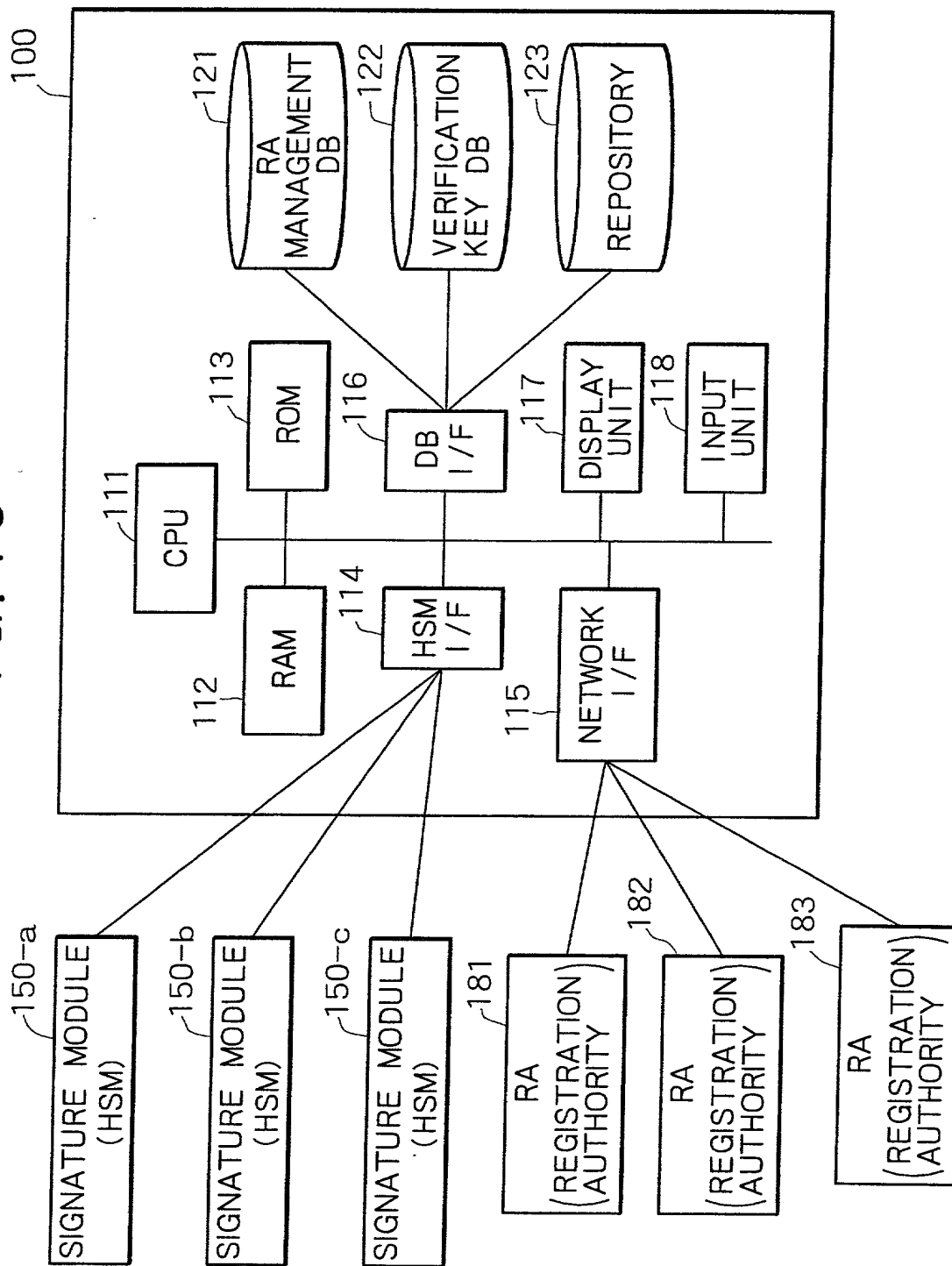


FIG. 11

EXAMPLE OF RA MANAGEMENT DATABASE AT CA

RA ID	USAGE OF MULTIPLE- SIGNATURE ALGORITHM	SIGNATURE ALGORITHM	KEY LENGTH	PARAMETERS	LOAD DISTRIBUTION	HSM IN USE
RA0001	X	RSA	1024 bits	—	X	001
RA0002	X	RSA	2048 bits	—	O	002, 003, 004
RA0003	O	RSA	512 bits	—	X	005
RA0003	O	ECDSA	160 bits	p=XX,...	X	101
RA0004	O	RSA	1024 bits	—	X	006
RA0004	O	RSA	2048 bits	—	X	007
RA0004	O	ECDSA	192 bits	p=YY,...	X	102
RA0004	O	ECDSA	224 bits	p=ZZ,...	X	103

FIG.12

VERIFICATION KEY DATABASE





HSM ID	SIGNATURE ALGORITHM	KEY LENGTH	PARAMETERS	VERIFICATION KEY
201	RSA	2048 bits	—	
201	RSA	1024 bits	—	
202	ECDSA	160 bits	p=XX,...	
202	ECDSA	192 bits	p=YY,...	

FIG. 13

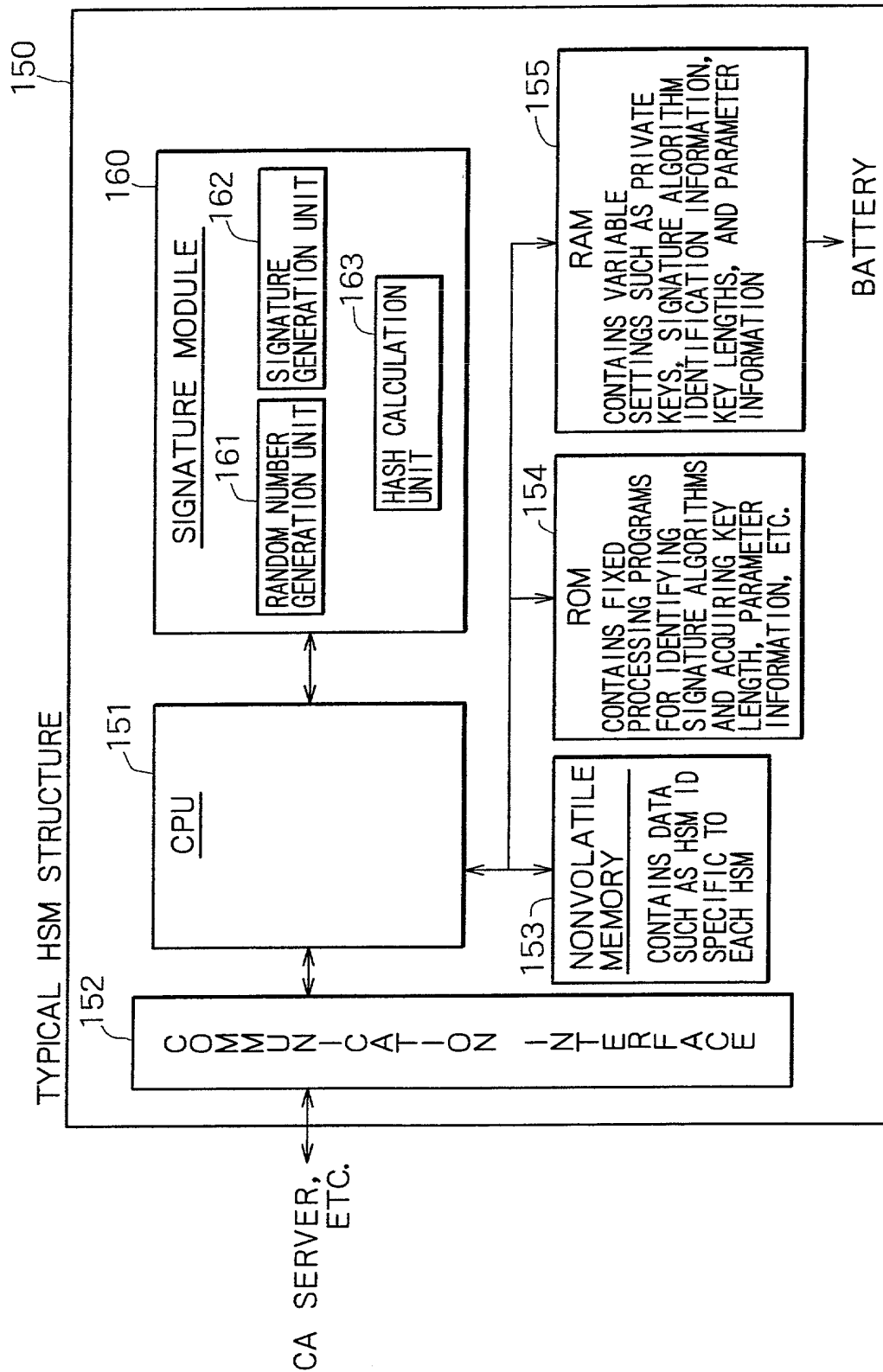


FIG. 14

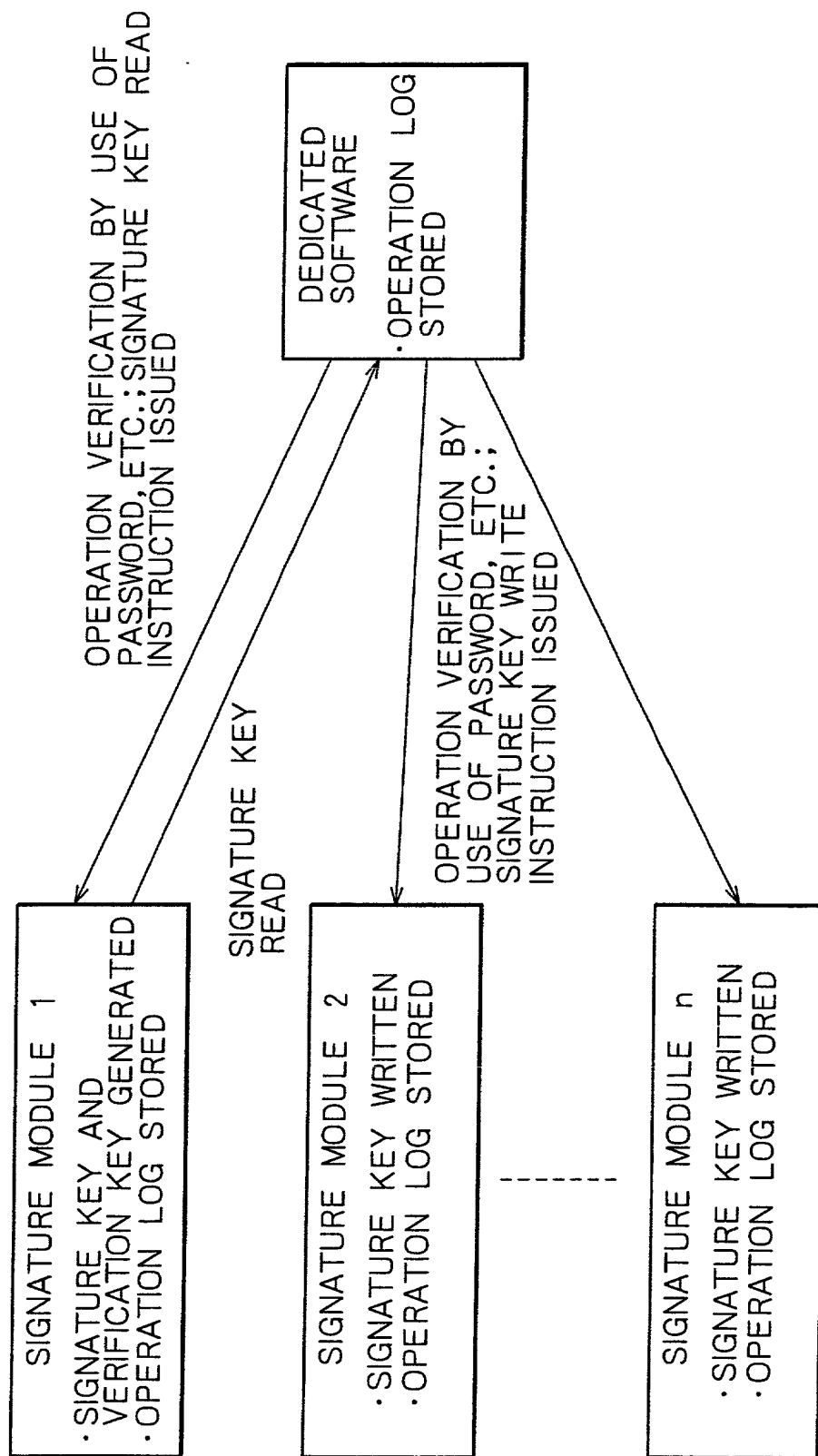


FIG. 15

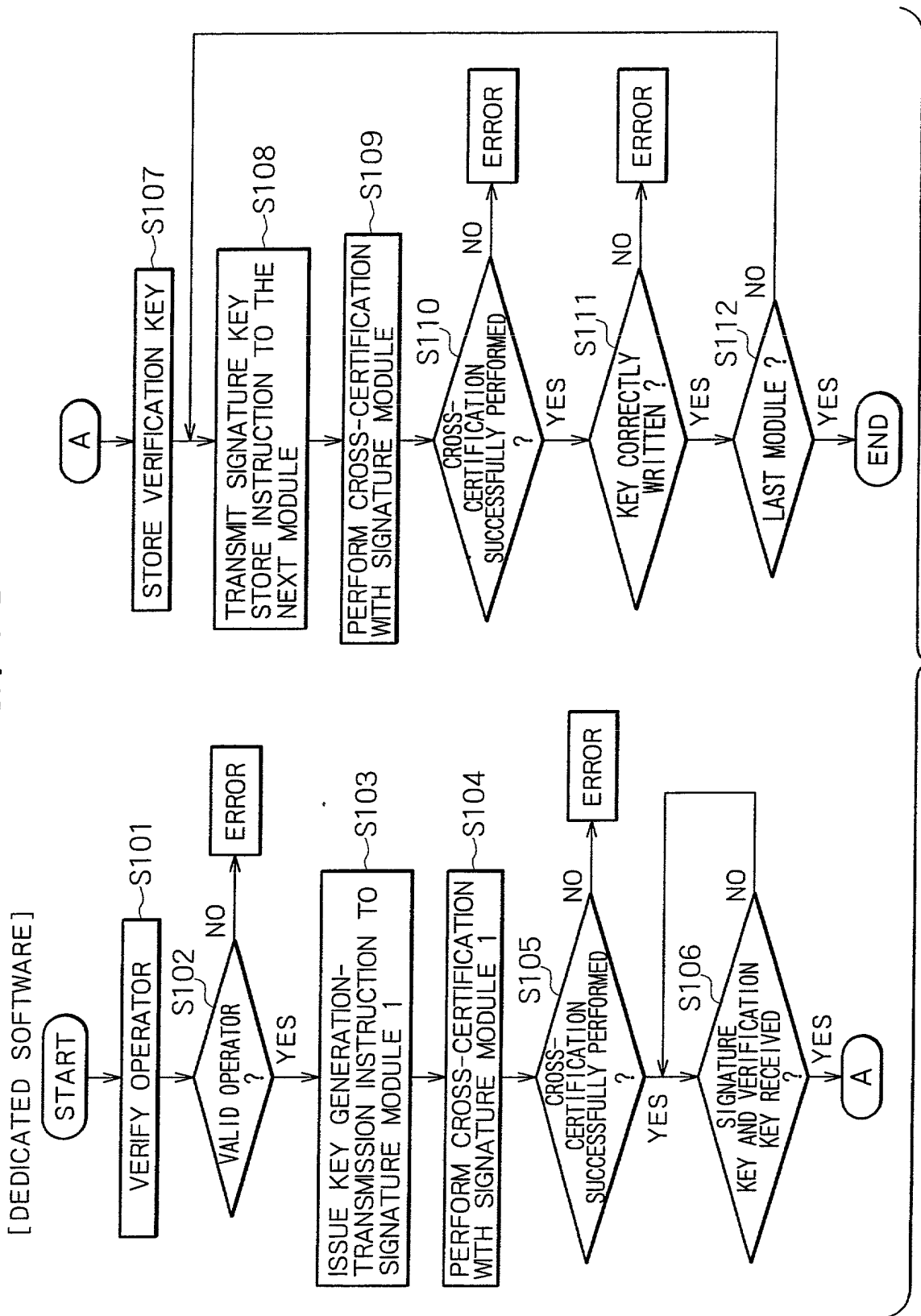


FIG. 16

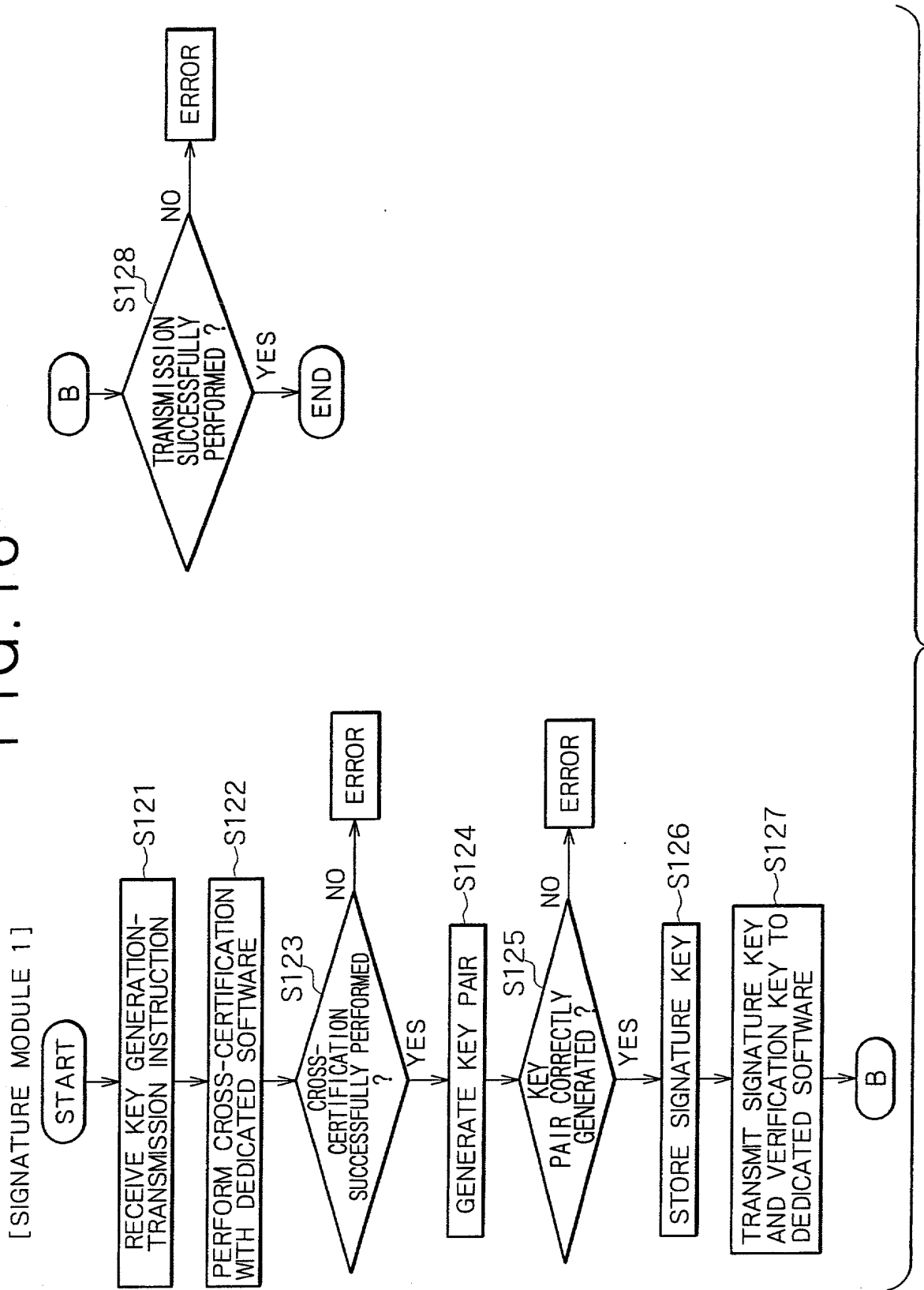


FIG. 17

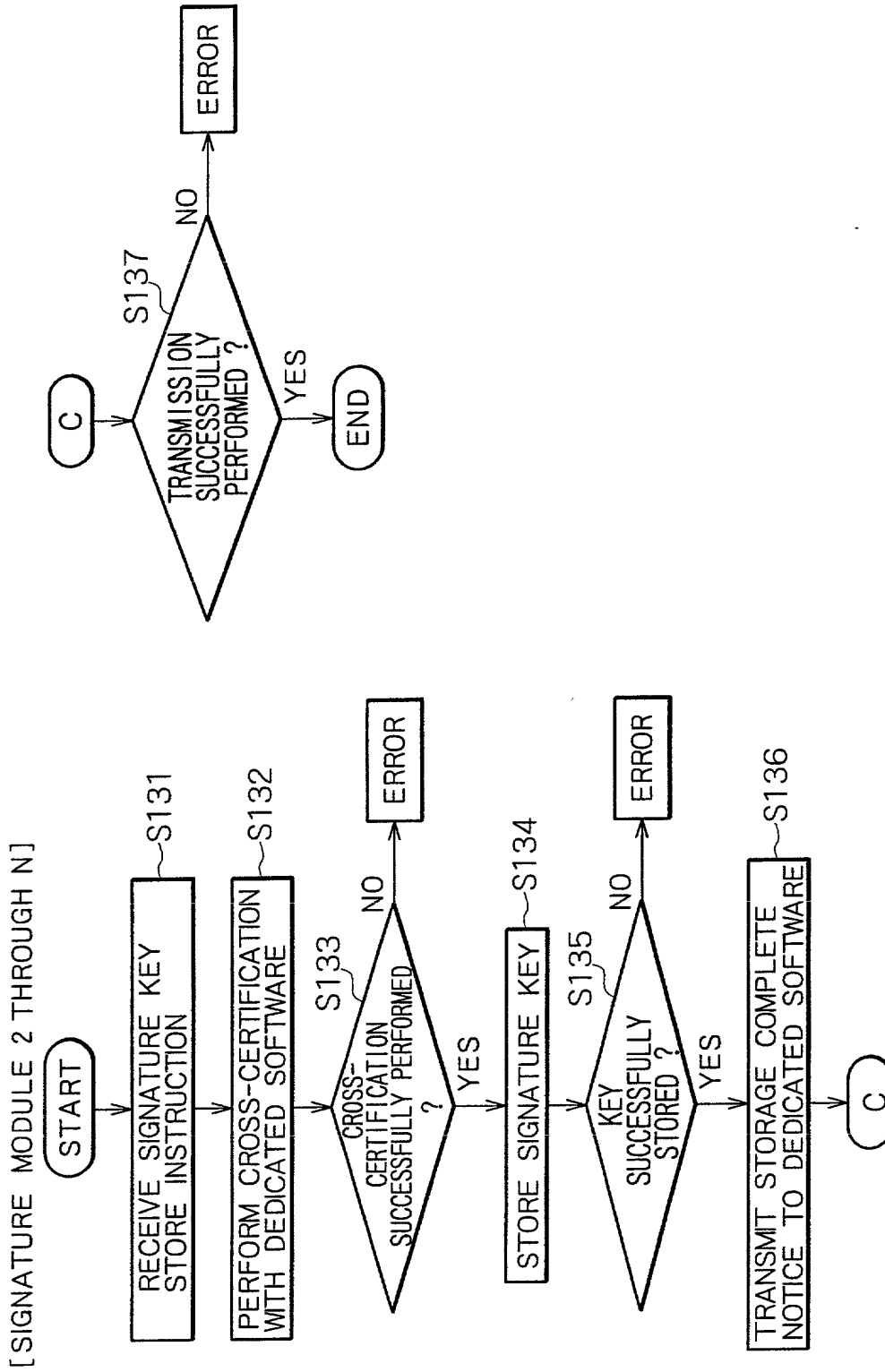


FIG. 18

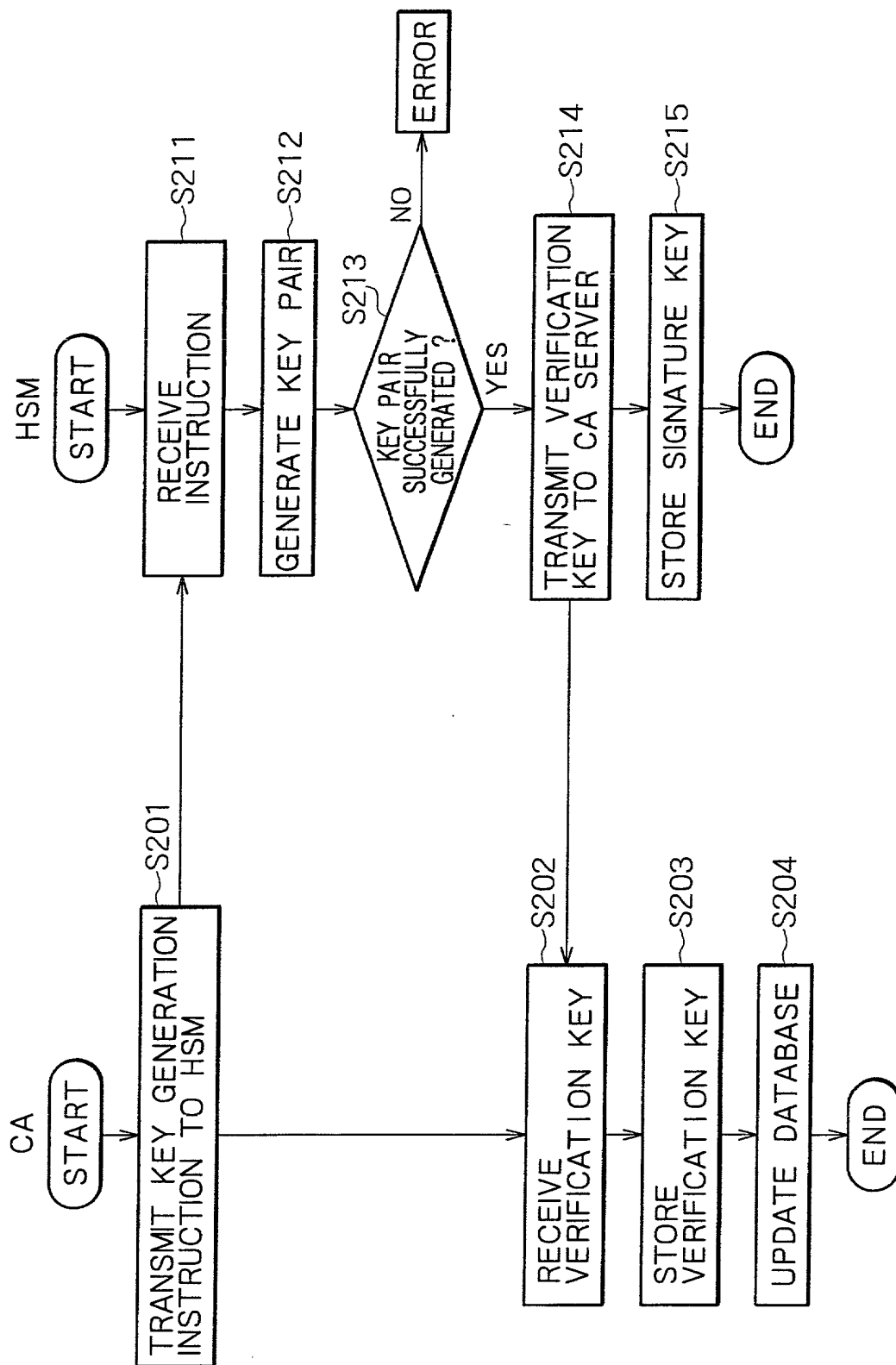


FIG. 19

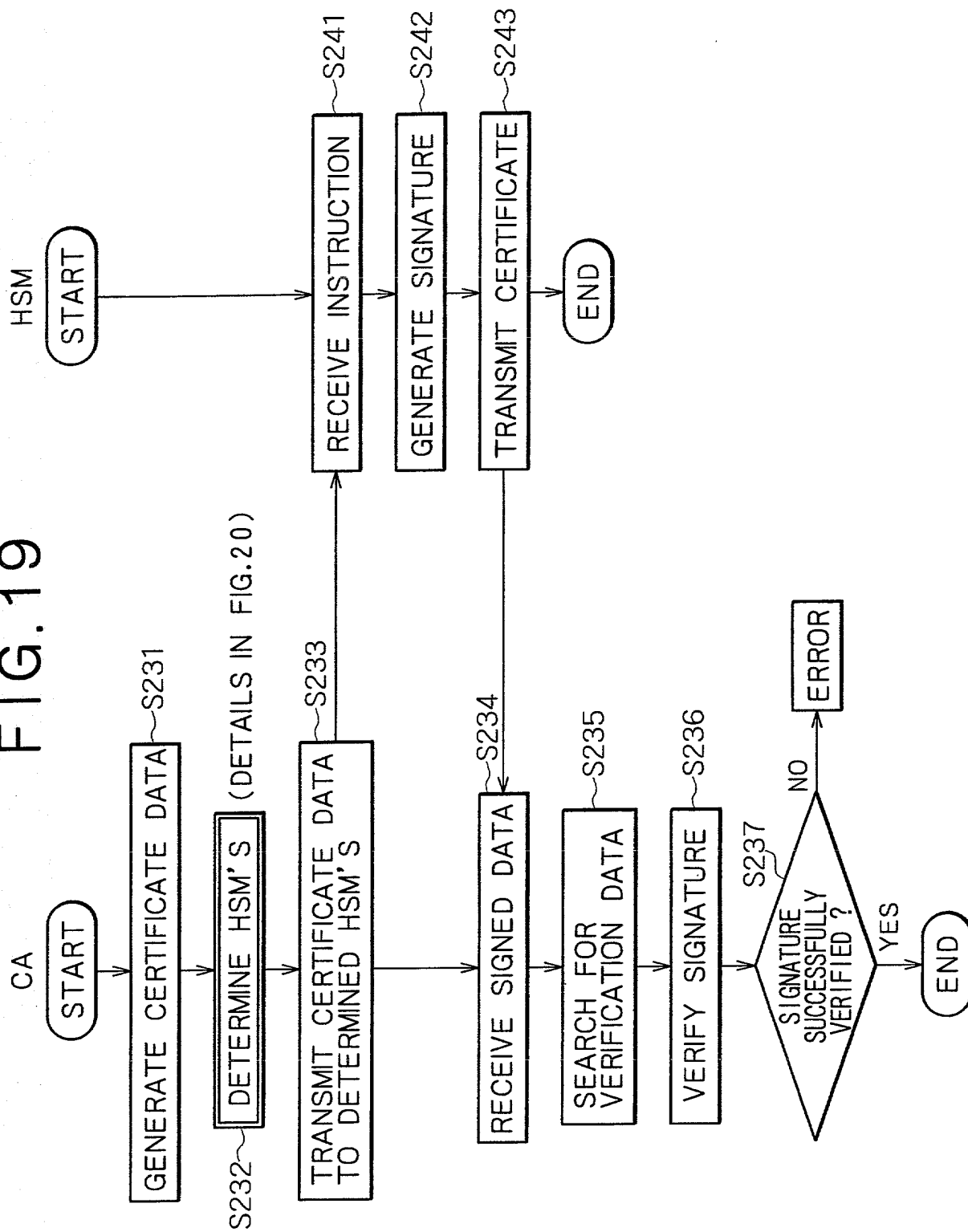


FIG. 20

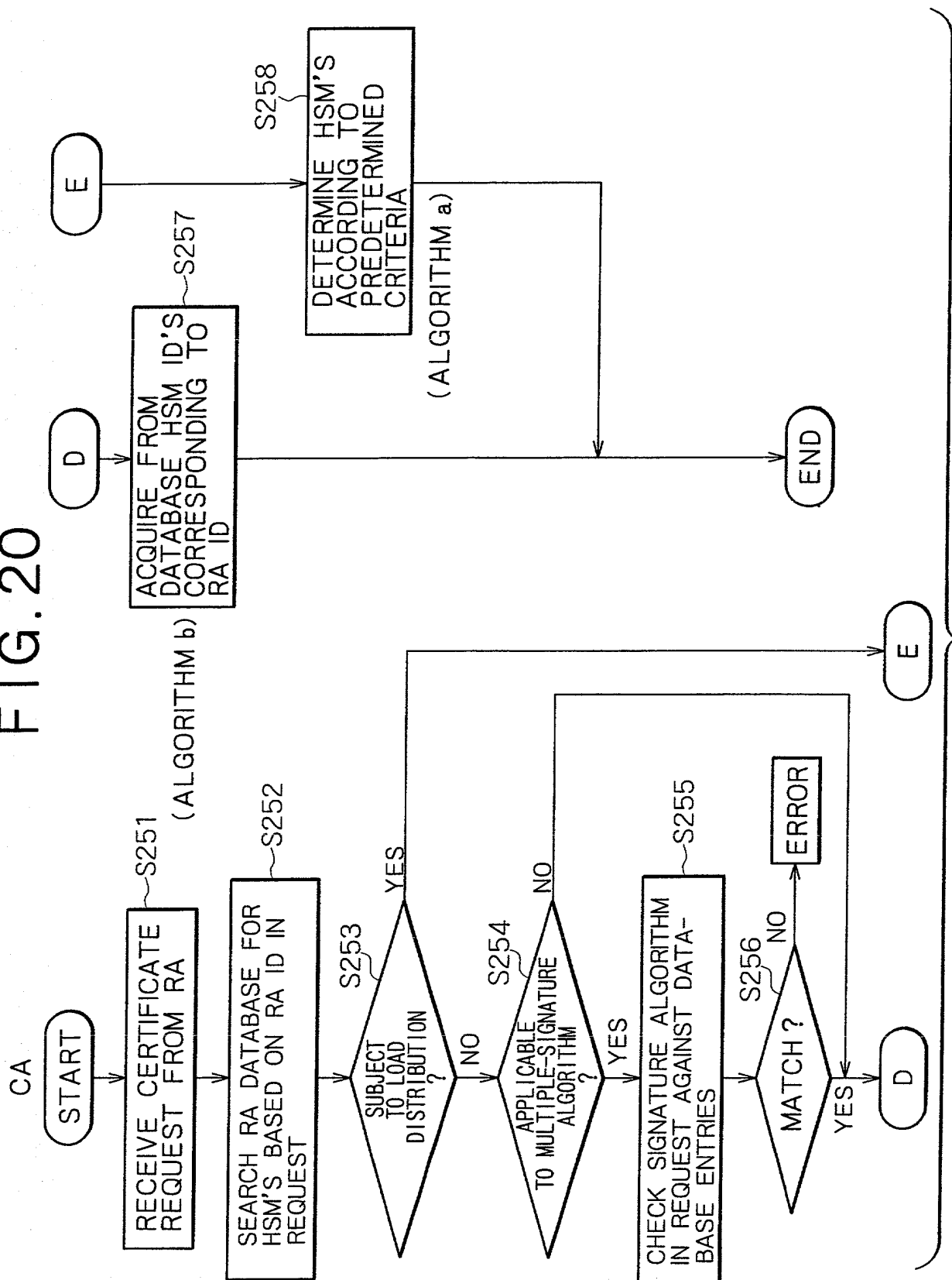
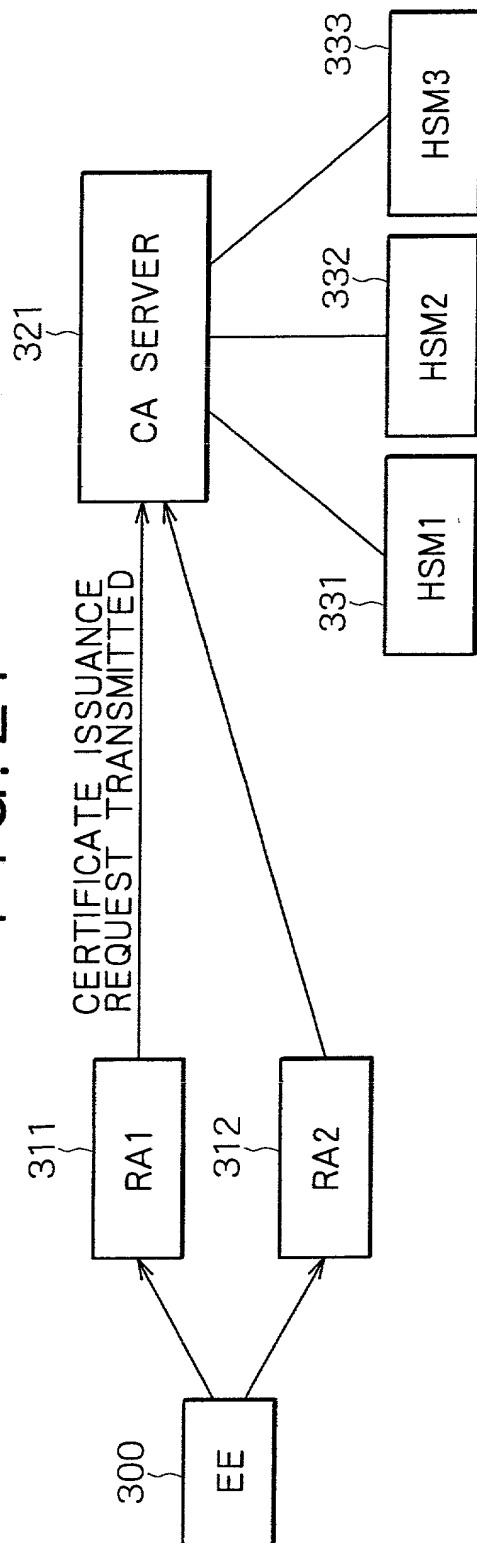


FIG. 21



(a) RA MANAGEMENT DATABASE

RA ID	USAGE OF MULTIPLE-SIGNATURE ALGORITHM	SIGNATURE ALGORITHM	KEY LENGTH	PARAMETERS	LOAD DISTRIBUTION	HSM IN USE
RA1	X	RSA	1024 bits	—	X	HSM1
RA2	O	RSA	2048 bits	—	X	HSM2
RA2	O	ECDSA	192 bits	p=XX,...	X	HSM3
RA2	O	ECDSA	192 bits	p=YY,...	X	HSM3

(b) VERIFICATION KEY DATABASE

HSM ID	SIGNATURE ALGORITHM	KEY LENGTH	PARAMETERS	VERIFICATION KEY
HSM1	RSA	1024 bits	—	◇—π
HSM2	RSA	2048 bits	—	◆—π
HSM3	ECDSA	192 bits	p=XX,...	△—π
HSM3	ECDSA	192 bits	p=YY,...	◀—π

FIG. 22 4. HSM'S DETERMINED BY REFERRING TO RA MANAGEMENT DATABASE

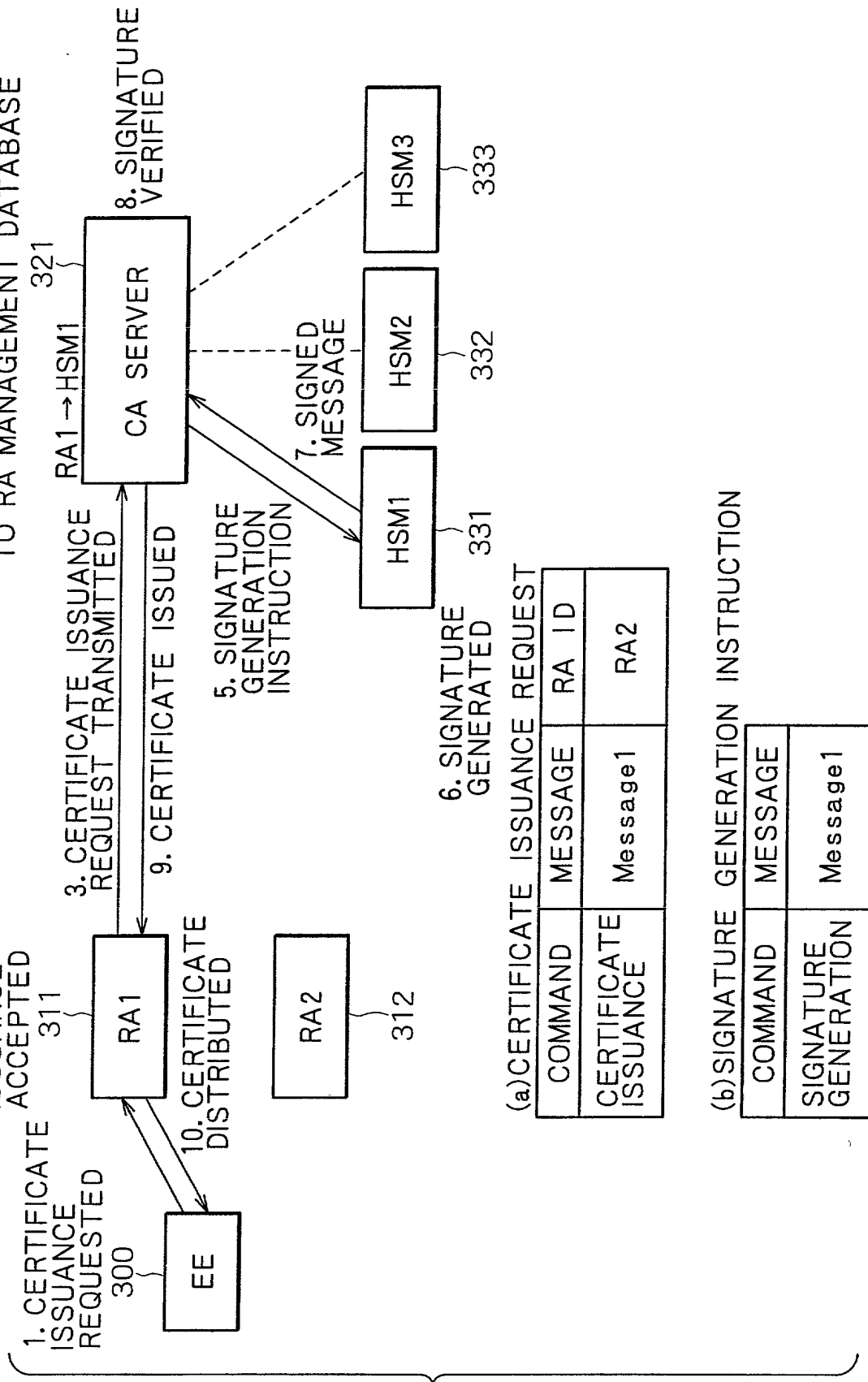
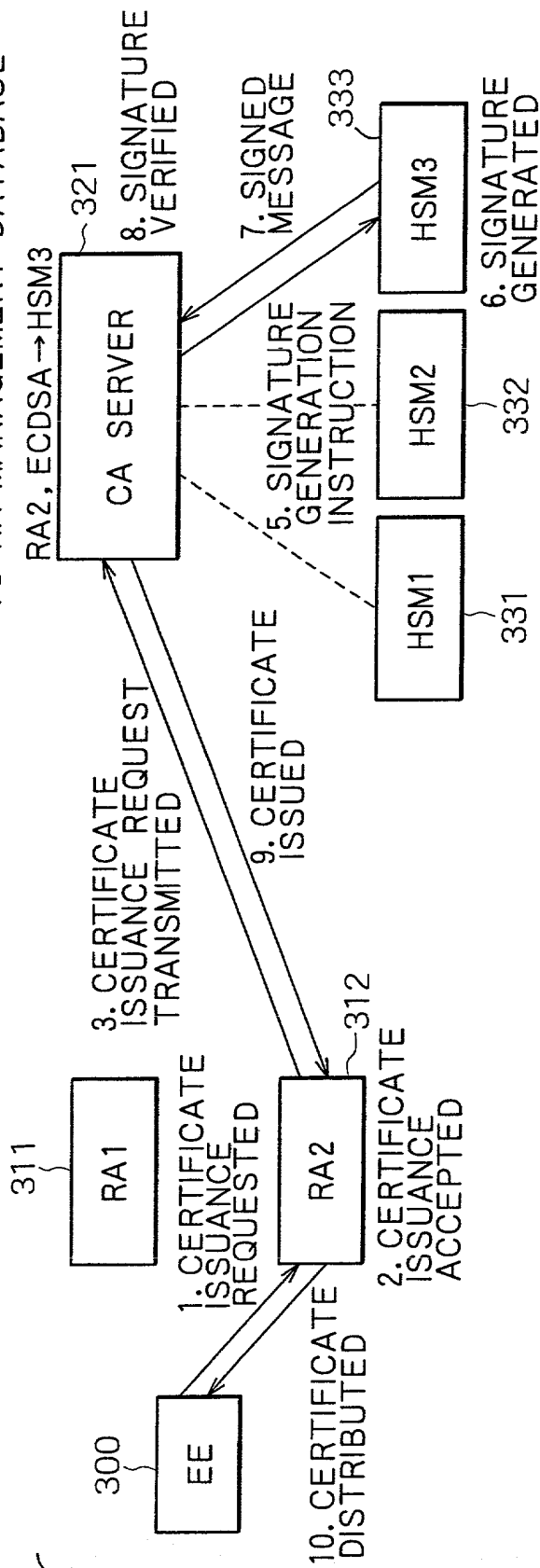


FIG. 23

4. HSM'S DETERMINED BY REFERRING TO RA MANAGEMENT DATABASE



(a) CERTIFICATE ISSUANCE REQUEST

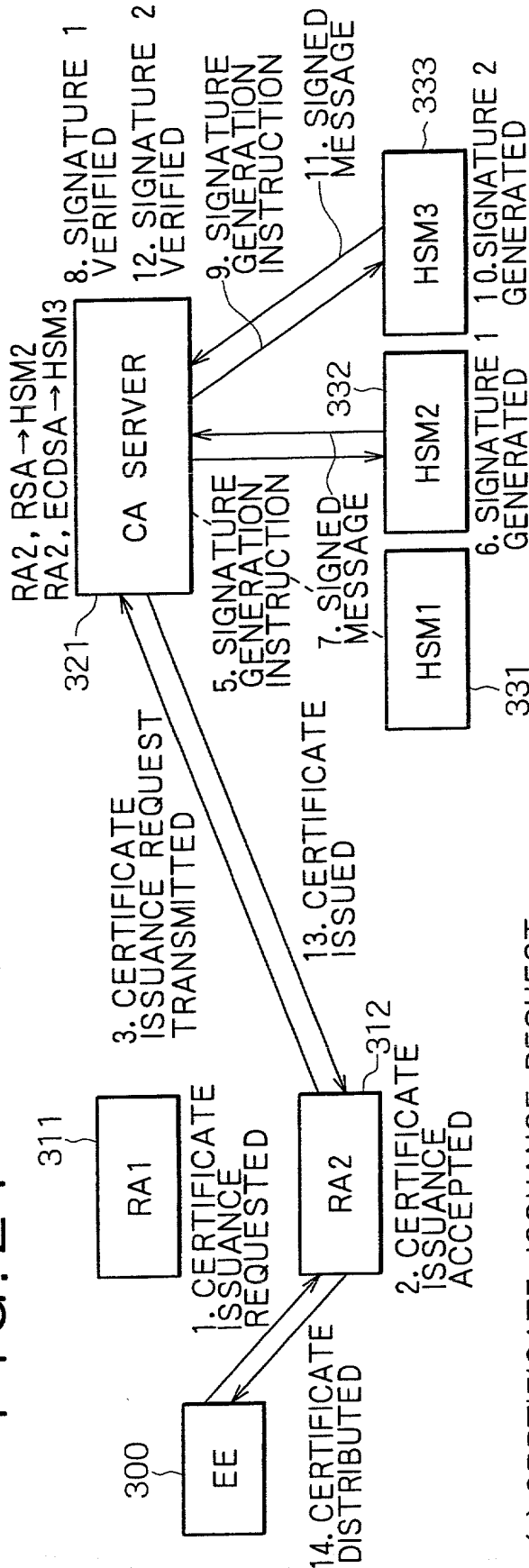
COMMAND	MESSAGE	RA ID	SIGNAL ALGORITHM	KEY LENGTH	PARAMETERS
CERTIFICATE ISSUANCE	Message2	RA2	ECDSA	192 bits	p=XX,...

(b) SIGNATURE GENERATION INSTRUCTION

COMMAND	MESSAGE	KEY LENGTH	PARAMETERS
SIGNATURE GENERATION	Message2	192 bits	p=XX,...

FIG. 24

4. HSM'S DETERMINED BASED ON CERTIFICATE ISSUANCE REQUEST AND RA MANAGEMENT DATABASE



(a) CERTIFICATE ISSUANCE REQUEST

COMMAND	MESSAGE	RA ID	SIGNATURE ALGORITHM 1	KEY LENGTH	SIGNATURE ALGORITHM 2	KEY LENGTH	PARAMETERS
CERTIFICATE ISSUANCE	Message3	RA2	RSA	2048 bits	ECDSA	192 bits	p=XX,...

(b) SIGNATURE GENERATION INSTRUCTION

COMMAND	MESSAGE	KEY LENGTH
SIGNATURE GENERATION	Message3	2048 bits

(c) SIGNATURE GENERATION INSTRUCTION

COMMAND	MESSAGE	KEY LENGTH	PARAMETERS
SIGNATURE GENERATION	Message3	192 bits	p=YY,...

FIG. 25

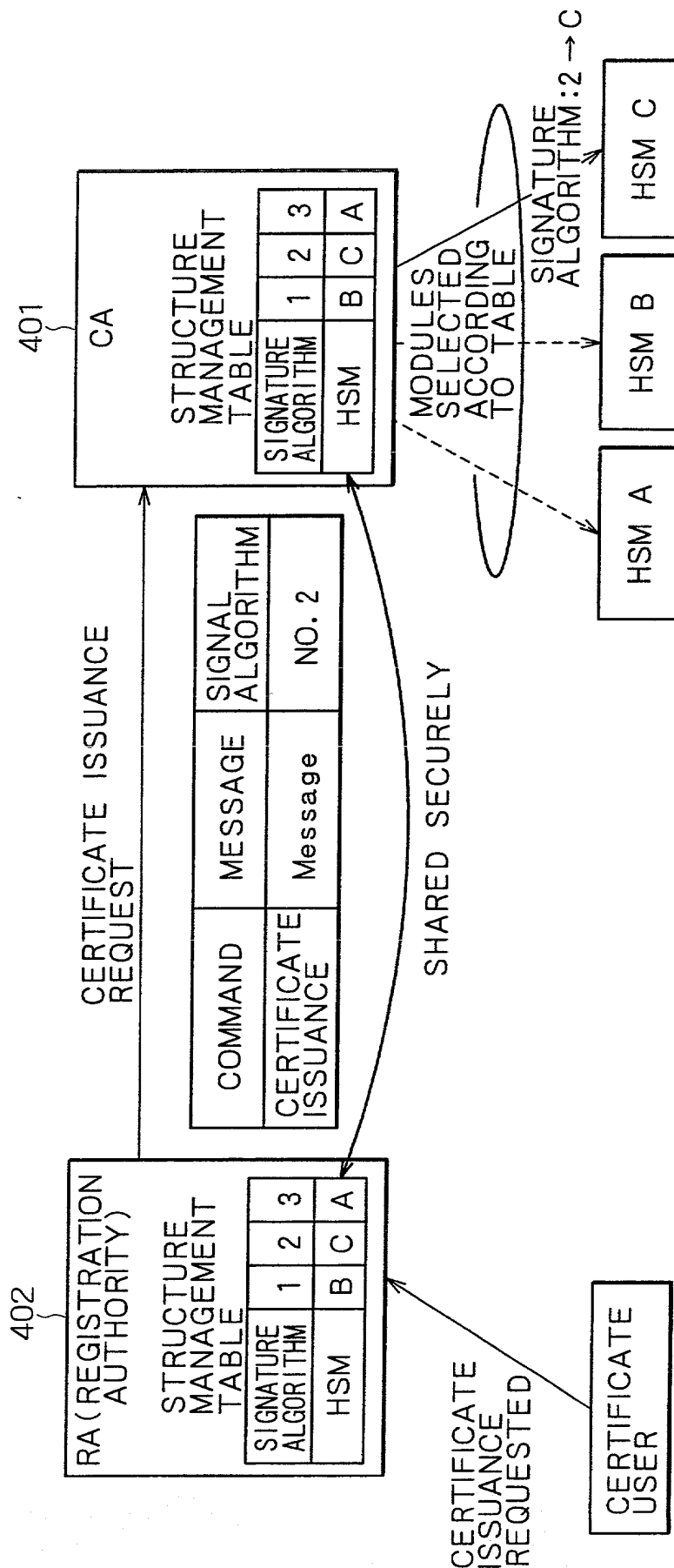


FIG. 26

